UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,316	10/15/2003	Peter L. Montgomery	MS1-1648US	8266

22801 7590 03/27/2007
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	03/27/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/27/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	**Application No.** 10/686,316	**Applicant(s)** MONTGOMERY, PETER L.	
	Examiner Shin-Hon Chen	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☒ Claim(s) *6,11,13 and 24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *3/17/06*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-24 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding independent claims 1, 7, 12, 15 and 20, the claimed invention as a whole must accomplish a practical application and must produce a useful, concrete, and tangible result. See MPEP 2106. In this instance, the claimed invention merely recites a method of "performing Montgomery multiplication" and the claimed limitations seem to be directed to an abstract idea without limitation to a practical application because the claim merely recites process of mathematical formula without producing tangible result.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-5, 7-10, 12, 15-21 and 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Posch et al. "RNS-Modulo Reduction Upon a Restricted Base Value Set and its Applicability to RSA Cryptography" (hereinafter Posch).

5. As per claim 1, Posch discloses a computer system comprising: a memory and a processor that supports SIMD instructions, the processor being configured to perform Montgomery multiplication using SIMD instructions (Posch: page 638: left column lines 11-25: SIMD instruction to perform Montgomery multiplication: (a^b mod n) in parallel fashion).

6. As per claim 2, Posch discloses the system of claim 1. Posch further discloses wherein the processor is executing a cryptographic function and the Montgomery multiplication is used to computer exponentiations in the cryptographic function (Posch: page 638: left column lines 11-25: SIMD instruction to perform exponentiation: a^b mod n).

7. As per claim 3, Posch discloses the system of claim 1. Posch further discloses wherein the processor maintains two arrays to hold intermediate computations from the Montgomery multiplication, and the SIMD instructions are used to simultaneously update the two arrays (Posch: page 640 right column lines 7-14: inherent parallelism in processing the sets RNS1 and RNS2).

8. As per claim 4, Posch discloses the system of claim 1. Posch further discloses wherein the Montgomery multiplication involves a first multiplication of an input array and a second

multiplication of a modulus array, and the SIMD instructions are used to perform simultaneously the first and second multiplications (Posch: page 641 left column figure 1: Mongtomery reduction in two multiplications).

9. As per claim 5, Posch discloses the system of claim 1. Posch further discloses wherein the Montgomery multiplication has a loop of instructions, and each iteration of the loop involves, excepting copy operations, using no more than eight SIMD instructions (Posch: page 641 left column figure 1: left than eight instructions are performed).

10. As per claim 7, Posch discloses a processing system comprising: a processor having a set of registers, the processor being configured to support SIMD instructions; and a set of SIMD instructions, executable by the processor, to perform Montgomery multiplication: montmul(A, B)=rem((AB-qN)/R, N), where q=rem(AB N', R). where A and B are integers, q is a quotient, N is a modulus, R is an integer that is coprime to modulus N, and N' is an integer such that N N'.ident.1 (mod R) (Posch: page 638 left column: lines 11-25: SIMD instruction to perform Montgomery multiplication; page 639 right column: Montgomery's algorithm).

11. As per claim 8, Posch discloses a processing system of claim 7. Posch further discloses wherein the SIMD instructions comprise a single SIMD instruction that simultaneously performs part of the multiplications AB and qN (Posch: page 641 left column: figure 1).

12. As per claim 9, Posch discloses a processing system of claim 7. Posch further discloses wherein the integer B and the modulus N are implemented as arrays, and at least one SIMD instruction is used to update a first array T.sub.1 with multiples of B for computing AB and to update a second array T.sub.2 with multiples of N for computing qN (Posch: page 641 left column figure 1: parallel processing of Montgomery reduction).

13. As per claim 10, Posch discloses a processing system of claim 9. Posch further discloses wherein a single SIMD instruction is used to update the first array T1 and the second array T2 simultaneously (Posch: page 641 left column figure 1).

14. As per claim 12, Posch discloses a computer readable medium comprising computer-executable SIMD instructions that, when executed, direct a processor to perform Montgomery multiplication (Posch: page 638 left column lines 11-25: SIMD computes Mongtomery multiplication).

15. As per claim 15, Posch discloses a method for computing Montgomery multiplication: montmul(A, B)=rem((AB-qN)/R, N), where q=rem(AB N', R). where A and B are integers, q is a quotient, N is a modulus, R is an integer that is coprime to modulus N, and N' is an integer such that N N'.ident.1 (mod R) (Posch: page 639 right column: montgomery reduction; page 640 left column (7): $z = abP^{-1}$ mod D), the method comprising: iteratively performing, for each digit of integer A from right to left: with array T.sub.1 being updated by a product of input B times the digit of integer A, determining what multiple of modulus N allows the updated arrays T2, T2 to

end with the same digit; multiplying the input B by the digit of integer A and multiplying the modulus N by the determined multiple; and updating the arrays T1, T2 (Posch: page 640 left column top portion: two RNS sets are necessary; page 641: left column figure 1: parallel processing of the algorithm).

16. As per claim 16, Posch discloses the method of claim 15. Posch further discloses wherein the performing comprises using SIMD instructions (Posch: page 638 left column lines 11-15: SIMD).

17. As per claim 17, Posch discloses the method of claim 15. Posch further discloses wherein the multiplying is performed by a single SIMD instruction (Posch: page 641 left column: figure 1).

18. As per claim 18, Posch discloses the method of claim 15. Posch further discloses initializing the arrays T.sub.1, T.sub.2 and the modulus N prior to said performing.(Posch: page 641 left column figure 1: two arrays are ready for parallel processing).

19. As per claim 19, Posch discloses the method of claim 15. Posch further discloses one or more computer readable media storing computer executable instructions that, when executed, perform the method as recited in claim 15 (Posch: page 638 left column: SIMD instructions).

20. As per claim 20, Posch discloses a method comprising: initializing a set of registers with values used in performing Montgomery multiplication (Posch: page 638 left column lines 11-25: utilize SIMD for Montgomery reduction); and computing the Montgomery multiplication with SIMD instructions on the values stored in the registers (Posch: page 641: left column).

21. As per claim 21, Posch discloses the method of claim 20. Posch further discloses wherein the computing comprises using the Montgomery multiplication to compute exponentiations in a cryptographic function (Posch: page 638 left column lines 11-15: modular exponentiation).

22. As per claim 23, Posch discloses the method of claim 20. Posch further discloses wherein the Montgomery multiplication has a loop of instructions, and each iteration of the loop is performed using not more than nine SIMD instructions (Posch: page 641 left column figure 1: less than 9 instructions).

Claim Rejections - 35 USC § 103

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

24. Claims 14 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Posch.

25. As per claim 14, Posch discloses the medium of claim 12. Posch further discloses that the instructions are executed on a SIMD machine (Posch: page 638 left column lines 11-15). The examiner interprets that the SIMD machine is capable of executing SSE2 instructions because SSE2, Streaming "Single Instruction Multiple Data" Extensions 2, is one of the IA-32 SIMD instruction sets. SSE2 was first introduced by Intel with the initial version of the Pentium 4 in 2001. Therefore, it would have been obvious to one having ordinary skill in the art to utilize the SSE2 instruction set in executing mathematical instructions.

26. As per claim 22, Posch discloses the method of claim 20. Posch further discloses that the instructions are executed on a SIMD machine (Posch: page 638 left column lines 11-15). The examiner interprets that the SIMD machine is capable of executing SSE2 instructions because SSE2, Streaming "Single Instruction Multiple Data" Extensions 2, is one of the IA-32 SIMD instruction sets. SSE2 was first introduced by Intel with the initial version of the Pentium 4 in 2001. Therefore, it would have been obvious to one having ordinary skill in the art to utilize the SSE2 instruction set in executing mathematical instructions.

Allowable Subject Matter

27. Claims 6, 11, 13 and 24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and if written to overcome the rejection(s) under 35 U.S.C. 101, set forth in this Office action.

28. The following is a statement of reasons for the indication of allowable subject matter:

As per claim 6 and 24, the closest prior art of record (Posch) discloses utilizing SIMD for performing execution of Montgomery multiplication. However, Posch does not explicitly disclose SIMD instructions comprise two load instructions, one multiply instruction, two add instructions, one copy instruction, one bitwise AND instruction, one store instruction, and one shift instruction.

As per claim 11, Posch fails to disclose a first register holds elements of the B and N arrays; a second register holds an element of the first array T1 and an element of the second array T2; and a third register is used to hold results of the first array T1 being updated with a multiple of B and the second array T2 being updated with multiples of N. As

As per claim 13, Posch fails to disclose a first SIMD instruction to load elements of arrays B and N into a first register; a second SIMD instruction to load elements of arrays T1 and T2 into a second register; a third SIMD instruction to multiply an element in the array B by a first multiple and an element in the array N by a second multiple; fourth and fifth SIMD instructions to add results of the third SIMD instruction to the array elements loaded by the second SIMD instruction and to any carries saved from a previous iteration; sixth and seventh SIMD instructions to separate each output of the fifth SIMD instruction into two reduced size results, one that fits into the arrays T1 and T2 and another that represents a carry for a next iteration; and an eighth SIMD instruction to update an element of array T1 and an element of array T2, in memory.

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Ikeda et al. U.S. Pub. No. 20040015532 discloses modular exponentiation method using pipeline processes.

Shimbo et al. U.S. Pub. No. 20020126838 discloses modular exponentiation calculation utsing RNS representation.

Monier U.S. Pat. No. 5745398 discloses method of modular multiplication according to the montgomery method.

Smith U.S. Pat. No. 6202077 discloses SIMD instruction for computing modular exponentiation in extended precision.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100